

EXHIBIT 2

To: Osborn, Phillip L[Phillip.L.Osborn@ice.dhs.gov]
Cc: 'Boutros, Andrew (USAILN)'[Andrew.Boutros@usdoj.gov]
From: DerYeghiayan, Jared
Sent: Thur 8/15/2013 9:18:19 AM
Importance: Normal
Sensitivity: None
Subject: FW: Email SW
Categories: vpacept

[Karpeles Email SW - draft to J Ellis.pdf](#)

FYI, preparing to swear this out today.

Jared

Jared Der-Yeghiayan
Special Agent
HSI Chicago
Office- 630-574-4167
Mobile- 630-532-3253

-----Original Message-----

From: Turner, Serrin (USANYS) [Serrin.Turner@usdoj.gov]
Sent: Thursday, August 15, 2013 09:47 AM Eastern Standard Time
To: michael_brantley@nysd.uscourts.gov
Cc: DerYeghiayan, Jared; Tarbell, Christopher W. (FBI)
Subject: Email SW

Michael –

As discussed, please find attached an email SW application. I can be reached at 646-660-4815 or serrin.turner@usdoj.gov whenever the judge is ready to see us. Thanks very much.

Serrin Turner
Assistant United States Attorney
U.S. Attorney's Office, Southern District of New York
1 St. Andrew's Plaza
New York, New York 10007
Phone: 212-637-1946
Fax: 212-637-2429
Email: serrin.turner@usdoj.gov

UNITED STATES DISTRICT COURT

for the
Southern District of New York

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)
THE EMAIL ACCOUNTS "magicaltux@gmail.com" and) Case No.
"mark@tibanne.com" MAINTAINED BY GOOGLE, INC.)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

THE EMAIL ACCOUNTS "magicaltux@gmail.com" and "mark@tibanne.com" MAINTAINED BY GOOGLE, INC.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

SEE ATTACHED RIDER.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before August 16, 2013
(not to exceed 10 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

☒ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. _____
USMJ initials

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for ___ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: _____

Judge's signature

City and state: New York, NY

HON. RONALD L. ELLIS

Printed name and title

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

[illegible]

UNITED STATES DISTRICT COURT

for the
Southern District of New York

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address) Case No.
THE EMAIL ACCOUNTS "magicaltux@gmail.com")
and "mark@tibanne.com" MAINTAINED BY)
GOOGLE, INC.)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

located in the Northern District of California, there is now concealed (*identify the person or describe the property to be seized*):

SEE ATTACHED RIDER.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. §§ 841 & 846; 18 U.S.C. §§ 1956, 1960, & 2	narcotics conspiracy, money laundering, operating unlicensed money transmitting business

The application is based on these facts:

SEE ATTACHED RIDER

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jared DerYeghiayan, Special Agent, Immigration and Customs
Enforcement-Homeland Security Investigations

Printed name and title

Sworn to before me and signed in my presence.

Date: August 15, 2013

Judge's signature

City and state: New York, NY

HON. RONALD L. ELLIS

Printed name and title

3505-00208

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - -	x	
IN THE MATTER OF THE APPLICATION	:	
OF THE UNITED STATES OF AMERICA	:	<u>TO BE FILED UNDER SEAL</u>
FOR A SEARCH WARRANT FOR THE	:	
PREMISES KNOWN AND DESCRIBED AS	:	AFFIDAVIT IN SUPPORT
THE EMAIL ACCOUNTS	:	OF A SEARCH WARRANT
"magicaltux@gmail.com" and	:	
"mark@tibanne.com" MAINTAINED BY	:	
GOOGLE, INC.	x	
- - - - -		

SOUTHERN DISTRICT OF NEW YORK, ss.:

Jared DerYeghiayan, being duly sworn, deposes and says:

1. I am a Special Agent at Immigration and Customs Enforcement-Homeland Security Investigations ("ICE-HSI"). I have been a Special Agent with ICE-HSI for over two years. I am presently assigned to the ICE-HSI Electronic Crimes Task Force in Chicago, Illinois. My responsibilities include investigating offenses involving, among other things, narcotics trafficking and cybercrime.

2. I make this affidavit in support of an application for a warrant to search the e-mail accounts "magicaltux@gmail.com" ("SUBJECT ACCOUNT-1") and "mark@tibanne.com" ("SUBJECT ACCOUNT-2") (collectively, the "SUBJECT ACCOUNTS") maintained by Google, Inc. (the "Provider").

3. For the reasons detailed below, there is probable cause to believe that the SUBJECT ACCOUNTS contain evidence, fruits, and instrumentalities of narcotics trafficking and money

laundering, in violation of Title 21, United States Code, Sections 841 and 846, and Title 18, United States Code, Sections 1956, 1960, and 2 (the "SUBJECT OFFENSES"), as described in Attachment A to this Affidavit.

4. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers and civilian witnesses. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

BACKGROUND ON THE PROVIDER

5. Based on my training and experience, I have learned the following about the Provider:

a. The Provider offers e-mail services available free of charge to Internet users, under the domain name "gmail.com." The Provider also offers paid services through which users can obtain e-mail accounts that are hosted by the Provider but that can be associated with any domain name that the user controls - e.g., "johndoe@myowndomain.com."

b. The Provider maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information.

c. Subscribers may access their accounts on servers maintained or owned by the Provider from any computer connected to the Internet located anywhere in the world.

d. Any e-mail that is sent to or from a subscriber is stored in the subscriber's "mail box" on the Provider's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by the Provider. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the Provider's servers indefinitely. Such stored messages can include attachments such as documents, images, and videos.

e. Computers located at the Provider contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrants seek authorization solely to search the SUBJECT ACCOUNTS, following the procedures described herein and in Attachment A.

STATUTORY PROVISIONS

6. 18 U.S.C. § 2703(b)(1)(A) allows the government to compel disclosure of all stored content and records or other information pertaining to a subscriber of an electronic communications service provider (such as the Provider) - without notice to the subscriber - pursuant to a search warrant issued using the procedures described in the Federal Rules of Criminal Procedure. Such an order may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

THE INVESTIGATION

Background on the Silk Road Underground Website

7. This application stems from an ongoing investigation into an underground website used to sell illegal drugs known as "Silk Road" (the "Silk Road Underground Website"). The Silk Road Underground Website provides an infrastructure similar to well-known online marketplaces such as Amazon Marketplace or eBay, allowing sellers and buyers to conduct transactions online. However, unlike such legitimate websites, the Silk Road Underground Website is designed to facilitate illegal commerce by ensuring absolute anonymity on the part of both buyers and sellers.

8. The primary means by which the Silk Road Underground Website protects the anonymity of its users is by operating on the "TOR" network. The TOR network is a special network of computers distributed around the world designed to conceal the true Internet Protocol ("IP") addresses of the users of the network.¹ Every communication sent through the TOR network is bounced through numerous relays within the network, and wrapped in a layer of encryption at each relay, such that the end recipient of the communication has no way of tracing the communication back to its true originating IP address. In a similar fashion, the TOR network also enables websites to operate on the network in a manner that conceals the true IP address of the computer server hosting the website.

9. Another means by which the Silk Road Underground Website protects the anonymity of its users is by requiring all transactions to be paid for through the use of "Bitcoins." Bitcoins are a virtually untraceable, decentralized, peer-to-peer form of electronic currency having no association with banks or governments. In order to acquire Bitcoins in the first instance, a user typically must purchase them from a Bitcoin

¹ Every computer attached to the Internet is assigned a unique numerical identifier known as an Internet protocol or "IP" address. A computer's IP address can be used to determine its physical location and, in turn, to identify the user of the computer.

"exchanger." Bitcoin exchangers accept payments of currency in some conventional form (cash, wire transfer, etc.) and exchange the money for a corresponding amount of Bitcoins (based on a fluctuating exchange rate); and, similarly, they will accept payments of Bitcoin and exchange the Bitcoins for conventional currency. Once a user acquires Bitcoins from an exchanger, the Bitcoins are kept in an anonymous "wallet" controlled by the user, designated simply by a string of letters and numbers. The user can then use the Bitcoins to conduct anonymous financial transactions by transferring Bitcoins from his or her wallet to the wallet of another Bitcoin user. All Bitcoin transactions are recorded on a public ledger known as the "Blockchain"; however, the ledger only reflects the movement of funds between anonymous wallets and therefore cannot by itself be used to determine the identities of the persons involved in the transactions.

10. Those operating Silk Road charge a commission, in the form of Bitcoins, for all sales conducted through the site. The commission varies between 8 to 15 percent, depending on the total value of the transaction. (The higher the value of the transaction, the lower the commission.)

11. Since November of 2011, ICE-HSI has made over 70 individual purchases of controlled substances from various

vendors on the Silk Road Underground Website. The substances purchased have been various Schedule I and II drugs, including ecstasy, cocaine, heroin, LSD, and others. As of April 2013, 56 samples of these purchases have been laboratory-tested, and, of these, 54 have shown high purity levels of the drug the item was advertised to be on Silk Road. (Two of the samples tested negative for any controlled substance.) Based on the postal markings on the packages in which the drugs arrived, these purchases appear to have been filled by vendors located in over ten different countries, including the United States.

12. I have traced the Bitcoins that were used in these undercover purchases through the Blockchain, the public ledger reflecting the transfer of Bitcoins from one Bitcoin wallet to another. In doing so, I have found that Silk Road Underground Website appears to use a highly complicated system of Bitcoin wallets to control the movement of Bitcoins in and out of the website. In particular, the website uses a "tumbler" that mixes the funds from various wallets together, so as to make it very difficult to trace the funds from a particular transaction to a particular Bitcoin wallet. Based on my training and experience, this system was likely designed by someone with a high level of technical expertise concerning the operation of Bitcoins.

Background on Mark Karpeles and
His Suspected Role in Establishing Silk Road

13. Based on Internet searches I have conducted, the Silk Road Underground Website appears to have been established in early 2011. In particular, from visiting an online discussion forum about Bitcoins, located at bitcointalk.org, I know that on February 28, 2011, a user account was created on the bitcointalk.org forum under the username "silkroad." The postings made by this user are no longer accessible on bitcointalk.org. However, I have reviewed media articles from mid-2011 which report that, on March 1, 2011, the "silkroad" user posted the following message on the forum:

Hi everyone, Silk Road is into its third week after launch and I am very pleased with the results. There are several sellers and buyers finding mutually agreeable prices, and as of today, 28 transactions have been made!

For those who don't know, Silk Road is an anonymous online market.

Of course, it is in its infant stages and I have many ideas about where to go with it. But I am turning to you, the community, to give me your input and to have a say in what direction it takes.

What is missing? What works? What do you want to see created? What obstacles do you see for the future of Silk Road? What opportunities?

The general mood of this community is that we are up to something big, something that can really shake things up. Bitcoin and Tor are revolutionary and sites like Silk Road are just the beginning.

I don't want to put anyone in a box with my ideas, so I will let you take it from here ...

- Silk Road staff

14. The "silkroad" user's account at the bitcointalk.org forum includes a signature block, which contains a hyperlink to the website "silkroadmarket.org." This is not the address of the Silk Road Underground Website, but rather is the address of a site on the ordinary Internet. (Websites operating on TOR have complex domain names ending in ".onion" and can only be accessed through TOR browser software.) However, from reviewing archived versions of the silkroadmarket.org website,² I know that in early 2011 this website was used to publicize the Silk Road Underground Website and to explain how it could be accessed through TOR. For example, an archived capture of the silkroadmarket.org homepage from March 4, 2011 reflects that, at the time, the website stated as follows:

This is not the Silk Road, but you are close...

The Silk Road is an anonymous online market. Current offerings include Marijuana, Hash, Shrooms, LSD, Ecstasy, DMT, Mescaline, and more. The site uses the Tor anonymity network, which anonymizes all traffic to and from the site, so no one can find out who you are or who runs Silk Road. For money, we use Bitcoin, an anonymous digital currency.

Accessing the site is easy:

² The archived material is available at www.archive.org, a non-profit digital library of archived websites.

1. Download and install the Tor browser bundle
(Click here for instructions and non-windows users)
2. Open your new Tor browser
3. Go to: <http://ianxz6zefk72ulzz.onion>

. . .

* it takes about a minute for you to make the initial anonymous connection to the site, but afterward you should be able to browse more quickly.

So what are you waiting for? Get Tor and get to Silk Road!
We'll see you inside :)

-Silk Road staff

15. Later archived captures from the silkroadmarket.org website reflect that the site continued to be used by the administrators of the Silk Road Underground Website to inform Silk Road users of service outages and otherwise to provide updates on the status of the service. For example:

a. On June 5, 2011, the silkroadmarket.org website posted a message stating: "The Silk Road is currently closed to new visitors. This will be reviewed on July 1st and the site will possibly be reopened. Sorry for the inconvenience : (."

b. On June 18, 2011, the silkroadmarket.org website posted a message stating: "So the server went down unexpectedly today. This was very unnerving because we thought it had somehow been seized or something terrible like that. Fortunately it was just some kind of glitch and we were able to reboot. Everything has been backed up and is totally current, but we are not going

to turn the site back on for a couple of days while we work out a way to prevent such problems."

16. Archived captures of the silkroadmarket.org website show that it ceased operating as an outlet for information about the Silk Road Underground Website in or about April 2012.

17. Based on publicly accessible information from domaintools.com,³ I have learned the following:

a. The "silkroadmarket.org" domain name was registered on March 1, 2011 by a "Richard Page" at 11640 Gary Street, Garden Grove, California. This contact information appears to be entirely fictitious, as I have been unable to find any information on a "Richard Page" associated with this address in any law-enforcement or open-source databases. Based on my training and experience, I believe that whoever registered the "silkroadmarket.org" domain name used false identification information in order to conceal his association with the website.

b. From March 1, 2011 through April 13, 2012, the "silkroadmarket.org" domain name was controlled through the

³ Whenever a domain name or IP address is registered so that it can be accessed through the Internet, the registrant must provide certain information to Internet governance authorities, including the registrant's contact information (which is not verified, however). This registration information is stored in what is known as the "WHOIS" database and can be searched through various websites, including domaintools.com.

domain name server "xta.net." A domain name server is a server responsible for translating a domain name (e.g., "abc.com") to an IP address (e.g., "198.199.200.201") and redirecting users who type in the domain name to the computer with the corresponding IP address. The "xta.net" domain name server used to control the "silkroadmarket.org" domain name has, since January 13, 2010, been registered to the company "Mutum Sigillum LLC." The administrative and technical contact person listed for the company in the domain name registration information is Mark Karpeles ("KARPELES"), with an e-mail address of "magicaltux@gmail.com" - i.e., SUBJECT ACCOUNT-1.

c. From March 1, 2011 through March 30, 2011, the silkroadmarket.org domain name resolved to the IP address 174.120.185.75 ("IP Address-1"). That is, traffic to the website was directed during this time, through the xta.net domain name server, to IP Address-1, where the content of the silkroadmarket.org website was hosted. Based on records subpoenaed from a server-hosting company that maintains IP Address-1, I have learned that IP Address-1 was leased to KARPELES from December 18, 2009 through April 1, 2011. The records list KARPELES's e-mail address as "mark@tibanne.com" - i.e., SUBJECT ACCOUNT-2.

d. In searching registration records for other websites hosted at IP Address-1 in 2011, I discovered that the website "tuxtelecom.com" was also hosted at IP Address-1 from March 1, 2011 through March 30, 2011. The "tuxtelecom.com" domain name is registered to KARPELES in his own name.

e. The websites for both silkroadmarket.org and tuxtelecom.com were subsequently moved - repeatedly and simultaneously - to different IP addresses. Specifically, on March 30, 2011, the IP addresses for both silkroadmarket.org and tuxtelecom.com changed to 173.224.127.76 ("IP Address-2"). Both websites remained at that address until April 21, 2011, when they were both moved to the IP address 173.224.119.60 ("IP Address-3"). I believe this evidence shows that KARPELES controlled the silkroadmarket.org website along with the tuxtelecom.com website, and that he hosted them both at IP addresses he controlled.

18. According to KARPELES's publicly accessible page on "LinkedIn" - a professional networking site where users can post their resumes and other career information - KARPELES is an experienced computer programmer. KARPELES's resume on LinkedIn indicates that, from 2003 to 2010, he worked as a software developer at various companies, specializing in developing e-commerce websites. Based on my training and experience, I know

that this type of background would make KARPELES well-suited to operating an e-commerce site such as the Silk Road Underground Website.

19. Based on media articles and Japanese incorporation records, I know that, by at least early 2011, KARPELES acquired a Bitcoin exchanger service based in Japan known as "Mt. Gox." KARPELES continues to own Mt. Gox to this day and serves as its Chief Executive Officer. According to its website, Mt. Gox is the "world's largest and oldest Bitcoin exchange" and handles "over 80% of all Bitcoin trade." Based on my own familiarity with the market for Bitcoins, I know that Mt. Gox is in fact one of the largest Bitcoin exchangers in operation at the present time, if not the largest.

20. I have spoken with a confidential informant ("CI-1") who has worked for KARPELES within the past two years. According to CI-1, KARPELES operates bitcointalk.org - the same discussion forum where Silk Road was first publicized by the user "silkroad" in late February 2011. From visiting the forum, I know that the forum operates on a software platform known as "Simple Machines." From visiting the Silk Road Underground Website on TOR, I know that this same software platform is used to operate the discussion forums included on the Silk Road Underground Website itself. Based on my training and

experience, the Simple Machines forum software is not widely used by forum administrators. Thus, the fact that the software is used to operate both the discussion forum on bitcointalk.org and the discussion forum on Silk Road indicates that the forums were likely set up by the same administrator - that is, KARPELES.

21. Similarly, from visiting the tuxtelecom.com website - publicly registered to KARPELES, as described above - I know that the website includes a webpage containing a tutorial about how to make phone calls over the Internet. From reviewing the source code for the webpage, I know that it was constructed using "wiki" software - a type of software commonly used to create tutorials, "frequently asked questions" or "FAQ" pages, and similar content on websites. More specifically, the source code reflects that the webpage was constructed using a specific "wiki" software called "Mediawiki," and a specific version of this software, version 1.17.⁴ From reviewing the silkroadmarket.org website and the Silk Road Underground Website, I know that these websites also contain pages constructed using "wiki" software (such as FAQ pages). The

⁴ Software vendors commonly update their software in order to fix bugs and to add new features. Each version of the software is denoted by a higher version number, with larger decimal places representing more significant revisions. (E.g., version 2.34 would be a minor revision to version 2.33, while version 3.0 would be a major revision to any version in the 2.xx series.)

source code for these pages reflects that they were constructed using the same version of the same software used to create the "wiki" page on the tuxtelecom.com website - Mediawiki version 1.17. From reviewing the Mediawiki website, I know that the Mediawiki software is regularly updated and that many versions have been released over time. Thus, the fact that the exact same version of the software was used to create the "wiki" page on tuxtelecom.com and the "wiki" pages on silkroadmarket.org and the Silk Road Underground Website indicates, again, that the same administrator - KARPELES - was responsible for creating all three of these sites.

22. Based on the foregoing, I believe that KARPELES has been involved in establishing and operating the Silk Road website. In summary, the evidence shows that:

a. KARPELES controlled the domain name server and the IP addresses used to host the silkroadmarket.org website on the ordinary Internet. This website was used by the "Silk Road Staff" to publicize the existence of the Silk Road Underground Website on TOR and later to provide information to users about the status of the website.

b. Moreover, in early 2011, around the same time that Silk Road began operating, KARPELES acquired Mt. Gox. Given his ownership of this Bitcoin exchange business, KARPELES

had a strong motive to create a large underground marketplace where Bitcoins would be in high demand. The Silk Road website was uniquely well suited to this purpose, as it has generated a huge source of demand for Bitcoins. Indeed, as of April 2013, the total value of Bitcoins in circulation topped 1 billion dollars. Because there are few legitimate vendors who accept Bitcoins as payment, it is widely believed that the rise of Bitcoins has been driven in large part by their use on Silk Road.

c. KARPELES has the technical expertise and experience necessary in order to establish and operate a large commercial website such as the Silk Road Underground Website. The fact that the Silk Road website utilizes the exact same forum software as bitcointalk.org and the exact same "wiki" software as tuxtelecom.com - both websites directly linked to KARPELES - provides further evidence of KARPELES's involvement in administering Silk Road. Finally, the fact that the Silk Road Underground Website relies on a highly complex system for processing Bitcoins strongly suggests that it was designed by someone with extensive technical expertise related to Bitcoins - which KARPELES, being the owner and operator of a major Bitcoin exchange and Bitcoin discussion forum, clearly has.

23. Accordingly, I respectfully submit there is probable cause to believe that KARPELES has engaged in the SUBJECT OFFENSES. Specifically:

a. By establishing and helping to operate Silk Road, an underground narcotics-trafficking website, KARPELES has participated in a conspiracy to distribute narcotics and has aided and abetted the distribution of narcotics, in violation of Title 21, United States Code, Sections 841 and 846 and Title 18, United States Code, Section 2.

b. Further, by operating a Bitcoin exchanger service, Mt. Gox, while knowing that a large volume of its business derives from narcotics trafficking activity conducted through Silk Road, KARPELES has violated U.S. money-laundering laws. Specifically, KARPELES has violated Title 18, United States Code, Section 1956, which prohibits, among other things, knowingly transferring the proceeds of narcotics trafficking activity with the intent to promote the carrying on of such unlawful activity. See 18 U.S.C. § 1956(a)(1)(A) & (c)(3). KARPELES has also violated Title 18, United States Code, Section 1960, which prohibits a person from operating a money transmitting business that involves the transmission of funds the person knows to have been derived from a criminal offense or

are intended to be used to promote or support unlawful activity.
See 18 U.S.C. § 1960(b)(1)(C).

Request to Search the Subject Accounts

24. As described above, KARPELES used SUBJECT ACCOUNT-1 to register the domain name server used to route Internet traffic to the silkroadmarket.org website, and he used SUBJECT ACCOUNT-2 to lease the IP address where the silkroadmarket.org website was initially hosted. Based on records subpoenaed from Google, I have learned the following:

a. Both of the SUBJECT ACCOUNTS are maintained by Google. The subscriber listed for both accounts is KARPELES.

b. Both of the SUBJECT ACCOUNTS were active as of the date of the subpoena return, April 5, 2013. Indeed, on April 4, 2013 alone, the Google records reflect 234 logins to SUBJECT ACCOUNT-1 and 211 logins to SUBJECT ACCOUNT-2.

25. Based on my training and experience, I know that, when a user is required to provide an e-mail address to register an account with an electronic communications service provider, the provider typically sends the user a receipt at the e-mail address provided. Accordingly, I believe that, at a minimum, the SUBJECT ACCOUNTS will contain records of KARPELES registering the accounts associated with the domain name server and an IP address used to host the silkroadmarket.org website.

By tying KARPELES to Silk Road, these records would provide evidence of KARPELES' involvement in the SUBJECT OFFENSES.

26. By the same token, I believe that KARPELES has also used the SUBJECT ACCOUNTS to register other accounts he has used in connection with the SUBJECT OFFENSES. For example, the SUBJECT ACCOUNTS likely contain communications reflecting KARPELES' registration of IP Address-2 and IP-Address-3, where the silkroadmarket.org website was moved after initially being hosted at IP-Address-1.

27. Finally, based on my training and experience, I believe it is likely that KARPELES has worked with others in establishing and operating the Silk Road Underground Website. Indeed, the postings on the silkroadmarket.org site that KARPELES controlled are signed "The Silk Road Staff" and are written in the plural first person. Based on my training and experience, I know that those involved in cybercrime often communicate with their co-conspirators over e-mail. Accordingly, I believe it is likely that the SUBJECT ACCOUNTS will contain communications between KARPELES and the co-conspirators involved with him in committing the SUBJECT OFFENSES.

28. Accordingly, I respectfully submit that there is probable cause to believe that the SUBJECT ACCOUNTS will contain

evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, as described more fully in Section II of Attachment A.

SEARCH PROCEDURE

29. In order to ensure that agents search only the SUBJECT ACCOUNTS, the search warrant requested herein will be transmitted to the Provider's personnel who will be directed to produce the information described in Section II of Attachment A. Based on my training and experience with executing email search warrants, I know that, for practical and logistical reasons, service providers typically produce all stored emails associated with an email account for which a search has been authorized. Upon receiving a digital copy of all stored email and stored content associated with a given email account, law enforcement personnel will review this content information using various techniques, including but not limited to performing keyword searches and undertaking a cursory inspection of all information from the SUBJECT ACCOUNTS (analogous to searching file cabinets in an office to determine which paper evidence is subject to seizure), to determine which information, including emails, contains evidence or fruits of the SUBJECT OFFENSES, as specified in Section III of Attachment A.⁵

⁵ I know from my training and experience that keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text

CONCLUSION

30. Based on the foregoing, I respectfully request that the Search Warrant sought herein issue pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

Dated: New York, New York
August 15, 2013

Jared DerYeghiayan
Special Agent
Immigration and Customs Enforcement-
Homeland Security Investigations

Sworn to before me on
August 15, 2013

HON. RONALD L. ELLIS
UNITED STATES MAGISTRATE JUDGE

data, yet many types of files commonly associated with emails (including attachments such as images and videos) do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search merely because the information fortuitously does not contain the keywords being searched.

Attachment A

Property to Be Searched

This warrant applies to information associated with the following e-mail accounts:

magicaltux@gmail.com
mark@tibanne.com

(the "SUBJECT ACCOUNTS") stored at a premises owned, maintained, controlled, or operated by Google, Inc., which is headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 ("the Provider").

Particular Things to Be Seized

I. Search Procedure

This warrant will be faxed or e-mailed to the Provider's personnel, who will be directed to produce the information described in Section II below. Upon receipt of the production, law enforcement personnel will review the information to locate the items described in Section III below.

II. Information to be Produced by the Provider

The Provider is required to disclose the following information for each of the SUBJECT ACCOUNTS, to the extent that the information is within the Provider's possession, custody, or control:

a. All stored e-mail and other stored content information presently maintained in, or on behalf of, the SUBJECT ACCOUNTS, and all existing printouts from original storage of e-mail associated with the SUBJECT ACCOUNTS, including all header information associated with such e-mails;

b. All histories, profiles, and contact lists (or "buddy" lists, "Friends" lists, or similar lists), including e-mail addresses, screen names, and user IDs, associated with the SUBJECT ACCOUNTS;

c. All transactional information concerning activity associated with the SUBJECT ACCOUNTS, including internet protocol address logs;

d. All business records and subscriber information, in any form kept, concerning the SUBJECT ACCOUNTS, including applications, account creation date and time, all full names, screen names, and account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records; and

e. All records indicating the services available to subscribers of the SUBJECT ACCOUNTS.

III. Information to Be Seized by the Government

The information to be seized by the Government includes all information described above in Section II that contains or constitutes evidence, fruits, and instrumentalities of narcotics trafficking and money laundering, in violation of Title 21, United States Code, Sections 841 and 846, and Title 18, United States Code, Sections 1956, 1960, and 2 (the "SUBJECT OFFENSES"), including any evidence concerning the following:

a. The identity and location of the user of the SUBJECT ACCOUNTS (the "User");

b. Any phone numbers, e-mail accounts, computer servers, IP addresses, domain names, or other electronic communications facilities or accounts maintained or controlled by the User;

c. The User's training, experience, and expertise concerning computers, the Internet, digital currency, the TOR network, and encryption;

d. The User's involvement in operating a Bitcoin exchanger service;

e. The User's involvement in narcotics trafficking;

f. The User's intent to promote narcotics trafficking through operating a Bitcoin exchanger service or knowledge that the exchanger service is facilitating narcotics trafficking;

g. The User's awareness of anti-money laundering laws and any efforts to comply with or evade such laws;

h. Communications with co-conspirators;

i. Passwords, encryption keys, and other access devices that may be necessary to access any of the User's communications or data; and

j. Any other evidence of the SUBJECT OFFENSES.

SEALING ORDER

SERRIN TURNER affirms as follows:

1. I am an Assistant United States Attorney in the Office of Preet Bharara, United States Attorney for the Southern District of New York, and, as such, I am familiar with this matter and the instant application for a warrant under 18 U.S.C. § 2703 to obtain certain stored electronic communications and related records kept at premises owned, maintained, controlled, or operated by Google, Inc. (the "Provider").

2. In light of the confidential nature of this continuing criminal investigation, the Government respectfully requests that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, in order to avoid premature disclosure of the investigation which could inform potential criminal targets of law enforcement interest, resulting in the endangerment of law enforcement agents and others, except that the Government may without further Order of this Court provide copies of the warrant and affidavit as needed to personnel assisting it in the investigation and prosecution of this matter, and may disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

3. With respect to the return of the warrant and inventory to the Clerk of Court, the Government further requests the return be sealed as the target of the present investigation has not yet been charged and public filing of the return at this time would compromise an ongoing investigation into violations of criminal law.

4. In addition, because notification of the existence of this order will seriously jeopardize an investigation, I request that, pursuant to 18 U.S.C. Section 2705(b), the Court order the Provider not to notify any person of the existence of the warrant.

Dated: New York, New York
August 15, 2013

PREET BHARARA
United States Attorney
Southern District of New York

By: _____
SERRIN TURNER
Assistant United States Attorney
Southern District of New York

SO ORDERED:

HON. RONALD L. ELLIS
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK